

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-65438

(43)公開日 平成11年(1999) 3月5日

(51)Int.Cl.⁶

G 0 9 C 1/00

識別記号

6 1 0

F I

G 0 9 C 1/00

6 1 0 Z

6 1 0 B

審査請求 未請求 請求項の数5 O L (全 6 頁)

(21)出願番号 特願平9-230562

(22)出願日 平成9年(1997) 8月27日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 高橋 勝己

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72)発明者 飯田 全広

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

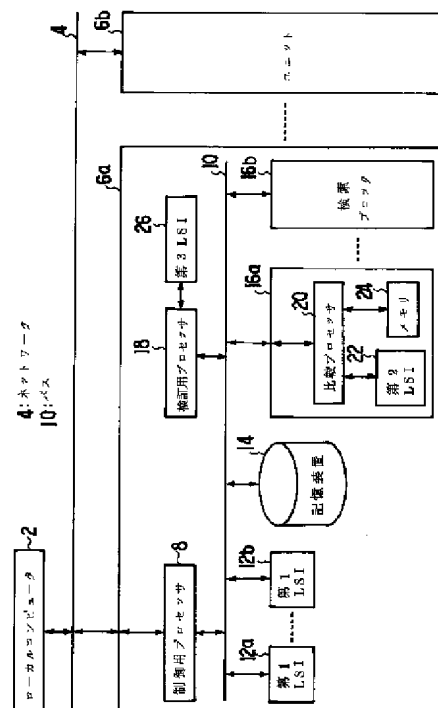
(74)代理人 弁理士 吉田 研二 (外2名)

(54)【発明の名称】 暗号強度評価装置

(57)【要約】

【課題】 従来技術で行われた暗号強度評価を行える装置を得ることを目的とする。

【解決手段】 暗号強度評価装置は、各ユニット6a、6bとこれを制御するローカルコンピュータ2とを有する。各ユニットは、表を生成する第1LSI12a、12bと、生成された表を格納する記憶装置14と、暗号文を加工する第2LSI22と、前記表を取り出して展開するメモリ24と、前記表と前記暗号文を加工した値とを比較する比較プロセッサ20と、この比較プロセッサ20から取り出した値を検証する検証用プロセッサ18と、検証のために前記表の生成時に用いた初期値を加工する第3LSI26と、これらを制御する制御用プロセッサ8と、を有する。この暗号強度評価装置を使用して、予め平文を想定して複数の表を作成し、暗号文を入手した後、暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求める。



【特許請求の範囲】

【請求項1】 暗号文を入手して、その鍵を求める暗号強度評価装置において、表を生成する第1LSIと、生成された表を格納する記憶装置と、暗号文を加工する第2LSIと、前記表を取り出して展開するメモリと、前記表と、前記暗号文を加工した値と、を比較する比較プロセッサと、この比較プロセッサから取り出した値を検証する検証用プロセッサと、検証のために前記表の生成時に用いた初期値を加工する第3LSIと、前記第1LSI、前記記憶装置、前記第2LSI、前記メモリ、前記比較プロセッサ、前記検証用プロセッサ及び前記第3LSIを制御する制御用プロセッサと、を有するユニットと、このユニットを制御するローカルコンピュータと、を有し、予め平文を想定して複数の表を作成し、暗号文を入手した後、暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めることを特徴とする暗号強度評価装置。

【請求項2】 前記第1LSI、前記第2LSI及び前記第3LSIを1つのLSIで実現することを特徴とする請求項1に記載の暗号強度評価装置。

【請求項3】 前記メモリは連想記憶メモリであり、前記比較プロセッサは、前記連想記憶メモリが一致した値があったと判定した場合、その値を取り出す回路で構成されることを特徴とする請求項1又は2に記載の暗号強度評価装置。

【請求項4】 前記回路を前記第2LSIに付加することを特徴とする請求項3に記載の暗号強度評価装置。

【請求項5】 前記第1LSI、前記第2LSI及び前記第3LSIは、強度評価する暗号を変更することができることを特徴とする請求項1〜4のうち、いずれか1項に記載の暗号強度評価装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号強度評価装置、特に予め平文を想定し、暗号文に対応する鍵を探索することにより、暗号強度を評価する暗号強度評価装置に関する。

【0002】

【従来の技術】従来の暗号方式として、米国の標準暗号である秘密鍵暗号方式DES(DataEncryption Standard)等が知られている。この暗号方式では、平文をある一定のブロックに区切り、ブロック単位で秘密鍵によって暗号化することにより、平文全体を暗号化することを特徴とする。この方式の暗号強度、即ち、解読のされにく

さは非常に高いとされるが、処理をブロック単位で行うため、平文の種類によっては、ブロック毎に一定の統計的性質を示す場合があり、これが、暗号強度を低下させる原因になる。また、暗号強度については、現在のところ特に定まった基準はなく、開発段階である。

【0003】従来の暗号強度評価については、『M.E.Hellman, "A cryptanalytic time-memory trade-off", IEEE Transaction on Information Theory, Vol.IT-26 No. 4』(以下、従来技術という)において記載された技術がある。この技術においては、予め平文から表を作成し、暗号文を加工しつつ、表との比較を繰り返すことにより、暗号強度を評価している。

【0004】

【発明が解決しようとする課題】しかしながら、上述の従来技術は、暗号強度の評価方法の技術を単に提示したに留まり、上記暗号強度評価方法を実現することができず、特に従来開示された評価方法をそのまま具体化すると、装置が大型、高価となり、また評価時間が長くなってしまいう問題があった。

【0005】本発明は以上のような問題点を解決するためになされたものであり、その目的は、従来技術で行われた暗号強度評価を行える装置を得ることを目的とする。

【0006】

【課題を解決するための手段】以上のような目的を達成するために、第1の発明に係る暗号強度評価装置は、暗号文を入手して、その鍵を求める暗号強度評価装置において、表を生成する第1LSIと、生成された表を格納する記憶装置と、暗号文を加工する第2LSIと、前記表を取り出して展開するメモリと、前記表と、前記暗号文を加工した値と、を比較する比較プロセッサと、この比較プロセッサから取り出した値を検証する検証用プロセッサと、検証のために前記表の生成時に用いた初期値を加工する第3LSIと、前記第1LSI、前記記憶装置、前記第2LSI、前記メモリ、前記比較プロセッサ、前記検証用プロセッサ及び前記第3LSIを制御する制御用プロセッサと、を有するユニットと、このユニットを制御するローカルコンピュータと、を有し、予め平文を想定して複数の表を作成し、暗号文を入手した後、暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めるものである。

【0007】第2の発明に係る暗号強度評価装置は、第1の発明において、前記第1LSI、前記第2LSI及び前記第3LSIを1つのLSIで実現するものである。

【0008】第3の発明に係る暗号強度評価装置は、第1又は第2の発明において、前記メモリは連想記憶メモリであり、前記比較プロセッサは、前記連想記憶メモリが一致した値があったと判定した場合、その値を取り出す回路で構成されるものである。

【0009】第4の発明に係る暗号強度評価装置は、第3の発明において、前記回路を前記第2LSIに付加するものである。

【0010】第5の発明に係る暗号強度評価装置は、第1～4の発明うち、いずれか1つの発明において、前記第1LSI、前記第2LSI及び前記第3LSIは、強度評価する暗号を変更することができるものである。

【0011】

【発明の実施の形態】以下、図面に基づいて本発明の好適な実施の形態について説明する。この際、DES暗号を用いて暗号強度の評価を行う暗号強度評価装置について説明する。

【0012】実施の形態1. 図1は、本発明の実施の形態1である暗号強度評価装置を示すブロック図である。暗号強度評価装置は、ローカルコンピュータ2と、ユニット6a、6bと、ユニット6a、6bとローカルコンピュータ2との間に接続されたネットワーク4と、を有する。

【0013】ローカルコンピュータ2は、装置全体の管理やユーザーとのインターフェイスを行う。ユニット6a、6bは、ローカルコンピュータ2からの指示により各処理を行うLSI等をまとめたものである。ネットワーク4は、データの送受信を行う。なお、各ユニット6a、6bは、ローカルコンピュータ2と並列接続されている。また、ユニットは図1に示す2個に限定されず、複数個ローカルコンピュータ2と並列接続されていてもよい。

【0014】各ユニット6a、6bは、ローカルコンピュータ2とネットワーク4を介して接続された制御用プロセッサ8を有し、この制御用プロセッサ8は、ユニット内を制御すると共に、その内部にはローカルなメモリが内蔵されている。この制御用プロセッサ8には、データ送受信用のバス10を介して、第1LSI12a、12b、記憶装置14、検索ブロック16a、16b及び検証用プロセッサ18が接続されている。

【0015】第1LSI12a、12bは、後述する解読事前処理にて、初期値から表の要素を作成する。記憶装置14には、上記表等が格納される。検索ブロック16a、16bは、解読処理において値の検索を行う。

【0016】この検索ブロック16a、16b内においては、比較プロセッサ20に第2LSI22及びメモリ24が接続されている。比較プロセッサ20は、メモリ24や第2LSI22を制御して、表の要素の検索を制御する。メモリ24では、表等を展開する。そして、第2LSI22では、暗号文を加工する。そして、展開された表と、暗号文を加工した値と、を比較プロセッサ20で比較する。

【0017】検証用プロセッサ18では、検索ブロック16a、16bが求めた解の候補を検証する。この検証用プロセッサ18には、第3LSI26が接続されてお

り、第3LSI26は検証用プロセッサ18が解の候補を検証する際に、値を加工する。

【0018】第2LSI22及び第3LSI26に内蔵されている暗号加工回路を図2に示す。図2において、暗号加工回路は、暗号化回路30と縮退化回路32とを有する。暗号化回路30では、入力された値の暗号化が行われる。縮退化回路32では、暗号化された値が縮退関数によって変形される。なお、これらの回路30、32の入力及び出力位置に、2入力1出力のセクタ34、36、38が配置されている。セクタ34は外部からの初期値と内部でループする際の値とを切り替え、セクタ36は暗号化の有無を切り替え、セクタ38は縮退関数による変形の有無を切り替える。

【0019】上述のように構成された暗号強度評価装置を使用して解読処理が行われるが、先ず、暗号文の入手前に表を作成する解読前処理について説明する。

【0020】解読前処理では、以下に示すような手順で各処理が行われる。

【0021】(1)ローカルコンピュータ2は、ユーザーの指示に従い、平文等の処理に必要なパラメータを決定する。

【0022】(2)ローカルコンピュータ2は、表作成の処理を各ユニット6a、6bに分配する。この際、ローカルコンピュータ2は平文、作成する表のタイプ(表タイプ番号が例えば100番から200番等)、表の要素数M、表作成のための加工繰り返し回数T等のパラメータを、ネットワーク4を介して、各ユニット6a、6b内の制御用プロセッサ8へ送る。

【0023】(3)制御用プロセッサ8は平文、表のタイプ、初期値、加工繰り返し回数T等のパラメータを第1LSI12a、12bへ送り、表の要素の作成を指示する。この際、初期値は表のタイプと、作成する要素の表における指標値(index番号)から生成する。例えば、初期値は、『表のタイプ番号 $\ll \log(M)$ + 指標値』の関係を満たす指標値等から作成できる。

【0024】(4)第1LSI12a、12bは、平文及び初期値を入力として、指定された表のタイプに応じた処理を行い、新しい値を生成する。第1LSI12a、12bは内部ループを持ち、上記新しい値を初期値の代わりに用いて、更に新しい値を生成する。そして、上述の過程をT回数繰り返す。要素作成が終了した場合、第1LSI12a、12bは制御用プロセッサ8に終了報告を行う。

【0025】(5)制御用プロセッサ8は終了報告を受け取った後、(4)でできた値を第1LSI12a、12bから取りだし、次の表の要素作成を第1LSI12a、12bに指示する。この指示は制御用プロセッサ8の処理が終了するまで繰り返される。

【0026】(6)制御用プロセッサ8は、表の全ての要素を受け取った場合、バス10を介して、その表を記

憶装置14に書き込む。この際、表の各要素から、その作成に用いられた初期値を求めるのに必要な情報も合わせて格納する。これらの処理を全ての表を作成するまで繰り返す。

【0027】(7)制御用プロセッサ8は全ての表の作成が終了した場合、その旨をローカルコンピュータ2に報告する。

【0028】(8)ローカルコンピュータ2は全てのユニット6a, 6bから終了報告を受け取るまで待機し、終了報告を受け取った場合、解読前処理は終了する。

【0029】次に、解読処理についての手順について、以下に説明する。

【0030】(1)ローカルコンピュータ2に暗号文が、入力される。

【0031】(2)ローカルコンピュータ2は、暗号文をネットワーク4を介して、各ユニット6a, 6bの制御用プロセッサ8に送る。

【0032】(3)制御用プロセッサ8は、暗号文を検索ブロック16a, 16bに送り、その後記憶装置14から表を取り出し、各検索ブロック16a, 16bに配布する。

【0033】(4)検索ブロック16a, 16bの比較プロセッサ20は暗号文と表とを受け取ると、それをメモリ24に格納する。

【0034】(5)比較プロセッサ20は第2LSI22に暗号文を入力として加工処理させ、新しい値を取り出し、表の各要素との比較を行う。この際、入力された値(暗号文)は、暗号化回路30を経由せず、縮退化回路32の加工処理のみ行われたものが新しい値となる。

【0035】(6)比較プロセッサ20は表の要素の中に一致するものがあれば、その要素の指標から、その要素が生成される際に用いられた初期値を求める。

【0036】(7)比較プロセッサ20は、新しい値を入力処理させ、さらに新しい値を取り出し、表の各要素との比較を行う。この際、入力された値は、暗号化及び縮退化の両方の加工処理を受けて生成された値となる。

【0037】(8)解読前処理における加工繰り返し回数Tだけ、(6)及び(7)を繰り返す。

【0038】(9)比較プロセッサ20は、上記(5)～(8)の処理において、一致する値の有無と、一致する値があった場合における要素に対応する初期値と、(5)の処理を0回目として上記一致した場合の加工処理は何回目の加工処理であるかと、に関する情報を制御用プロセッサ8に報告する。

【0039】(10)制御用プロセッサ8は一致した値が報告された場合、その初期値、検索に要した加工回数、平文、表のタイプ番号、表作成時の加工回数Tを検証用プロセッサ18に送る。また、一致した値の有無にかかわらず、記憶装置14から他の表を取り出し、検索ブロック16a, 16bに対して、上記(4)から(1

0)の加工処理を行う。そして、記憶装置14内に記憶されている全ての表に対して、上述の加工処理を行う。

【0040】(11)検証用プロセッサ18は、表作成時に行われた加工回数Tから、上記検索に要した加工回数を引いた処理回数値を求め、初期値、平文、表のタイプ番号及び処理回数値を第3LSI26に送る。

【0041】(12)第3LSI26は、初期値、平文、表のタイプ番号、処理回数値を受け取り、その値から1を引いた回数だけ加工処理を繰り返した結果と、最後にもう一度加工処理した結果と、を検証用プロセッサ18に送る。この際、前者は暗号化と縮退化の両方を経由したものであり、後者は暗号化のみを経由したものである。

【0042】(13)検証用プロセッサ18は、第3LSI26から受け取った値のうち、縮退化を経由しなかった値と、暗号文と、を比較する。比較した結果、値が一致した場合、1回分処理の少ない値を解読結果(暗号文の鍵)として、制御用プロセッサ8に報告する。値が一致しなかった場合、終了報告のみを報告する。

【0043】(14)制御用プロセッサ8は解読結果を受け取った場合、その値をネットワーク4を介して、ローカルコンピュータ2に報告する。一方、終了報告を受け取った場合には、他の検証すべき値を検証用プロセッサ18に送る。

【0044】(15)制御用プロセッサ8は全ての表の処理が終了した場合、ローカルコンピュータ2に対して、その終了報告を行う。

【0045】(16)ローカルコンピュータ2は解読結果(鍵)を受け取った場合、その値を表示すると共に、各ユニット6a, 6bに対し、処理の中止を指示する。また、解読結果を受け取らず、全てのユニット6a, 6bから終了報告を受け取った場合、鍵が発見できなかった旨を表示する。

【0046】以上の(1)から(16)の処理により、解読処理は終了する。

【0047】以上のようにして、実施の形態1に示された装置により、従来の暗号強度評価方法を実現することができる。

【0048】実施の形態2. 本発明の実施の形態2である暗号強度評価装置において、実施の形態1である暗号強度評価装置と異なる点は、比較プロセッサ20により、メモリ24に格納される表が異なる点にあり、必要な構成要素は実施の形態1と同一である。

【0049】実施の形態1では、比較プロセッサ20は第2LSI22から受け取った値と、表の各要素と、の比較をそのまま行っていた。このため、表の要素から初期値を求めるための変換テーブルのようなものが必要となる。そこで、実施の形態2では、実施の形態1の解読処理(4)でメモリ24に表を格納する際に、ソートやハッシュをおこなう。これにより、上記変換テーブルの

情報が付加された表がメモリ24に格納されて、比較時間を短縮することができる。上記ハッシュとしては、表の要素数をMとし、下位 $\log(M)$ ビットをハッシュ関数として取り出してアドレスとする方法や、事前に数ビットシフトしてから上記方法と同様に下位ビットをハッシュ関数として取り出す方法等がある。なお、ハッシュにおける値の衝突については、衝突したものをチェーンリストで実装する方法、衝突の際に2つめ以降の値を無視する方法、衝突のある表自体を無視する方法等により、衝突の影響を回避できる。

【0050】実施の形態3. 本発明の実施の形態3である暗号強度評価装置において、実施の形態2で示された装置と異なる点を以下に示す。実施の形態2では、解読処理(4)で表をメモリ24に格納する際に、ソートやハッシュを行ってから、メモリ24に格納していたが、本実施の形態では、解読前処理(6)の時点でソートやハッシュが行われ、この表が、記憶装置14に格納されている。この場合におけるソートやハッシュの仕方について、以下に示す。

【0051】(61)制御用プロセッサ8は表の値を比較プロセッサ20へ送る。

【0052】(62)比較プロセッサ20は表の値をメモリ24に展開し、これにソートやハッシュの変換処理を行う。そして、変換テーブルを含む表を作成して、これを制御用プロセッサ8に送る。

【0053】(63)制御用プロセッサ8は、受け取った新たな表の値を記憶装置14に格納する。このため、変換テーブル分、記憶装置14に必要な容量が増える。

【0054】そして、解読処理の際には、記憶装置14から表を取り出して、各処理をすることができる。

【0055】実施の形態3において、事前に数ビットシフトしてから下位ビットを取り出すハッシュを行う場合、シフトするビット数を調整することで、高い確率でハッシュ値の衝突を避けることができる。また、解読処理前に行っているため、衝突が避けられない表は削除し、別の表タイプ番号の表を作成(追加)することも可能である。

【0056】実施の形態4. 図1に示すように、実施の形態1の暗号強度評価装置では、制御用プロセッサ8と検証用プロセッサ18とを別々のものにしていたが、本実施の形態では、制御用プロセッサ8が検証用プロセッサ18の検証機能を有する。このため、検証用プロセッサ18を省略することができる。この際、第3LSI26は制御用プロセッサ8又はバス10に接続される。

【0057】実施の形態5. 実施の形態1の暗号強度評価装置では、第1LSI12a, 12bに1つの初期値を与えて値を生成しているが、本実施の形態では、1つのLSI12aに複数の初期値を与えて処理させる。この際、暗号化回路30や縮退化回路32には、その内部に複数のラッチを入れ、回路内の値を保持させ、動作周

波数を上げている。

【0058】本実施の形態5においては、ラッチ分だけ回路規模が大きくなるが、動作周波数を上げることができるので、LSI22, 26のスループットが向上する。

【0059】実施の形態6. 実施の形態6における暗号強度評価装置では、実施の形態1で別々のものであった第1LSI12a, 12bと第2LSI22とを、1つのLSIにまとめている。

10 【0060】これにより、例えば解読前処理も第2LSI22に行わせることで、第1LSI12a, 12bを省略することができる。但し、第1LSI12a, 12bに要求されている性能はスループット性能であり、第2LSI22に要求されている性能はレイテンシ性能である。また、解読前処理と、解読処理と、では処理量が異なる。このため、第1LSI12a, 12bと第2LSI22とを、共用させる範囲には制限がある。また、第3LSI26も第2LSI22と共用させることが可能である。

20 【0061】実施の形態7. 本実施の形態の暗号強度評価装置において、実施の形態1で示す暗号強度評価装置と異なる点は、メモリ24を連想記憶メモリにしている点にある。そして、連想記憶メモリが第2LSI22の出力値と表の要素とが一致したと判定した場合には、その値を取り出す回路で、比較プロセッサ20は構成されている。

【0062】これにより、実施の形態2で行われている表変換を行うことなく、第2LSI22の出力値の値と表の要素とが一致した場合には、ほぼ一定時間でそのアドレスを知ることができる。なお、表が1つの連想記憶メモリに格納できない場合には、比較プロセッサ20は、複数の連想記憶メモリに表を分割して格納し、第2LSI22の出力結果を各連想記憶メモリにブロードキャストすることで一致する値を探索する。

【0063】実施の形態8. 本実施の形態の暗号強度評価装置において、実施の形態1で示す暗号強度評価装置と異なる点は、メモリ24を連想記憶メモリにすると共に、比較プロセッサ20の機能を第2LSI22に埋め込んでいる点にある。

40 【0064】実施の形態7では比較プロセッサ20は、連想記憶メモリに第2LSI22の出力値を送る。そして、この値と表の要素とが一致した場合には、比較プロセッサ20は、その信号とアドレスとを受け取り、制御用プロセッサ8に報告しているだけである。このため、比較プロセッサ20を実現する回路は、比較的単純であり、第2LSI22に埋め込むことができる。

【0065】実施の形態9. 本実施の形態の暗号強度評価装置では、暗号化回路30について、DES暗号に暗号化する回路から、例えばFEAL暗号に暗号化する回路に変更することが可能である。このため、強度評価す

る暗号に応じて、暗号化回路30を変更すれば、どの暗号に対しても、暗号強度評価を行うことができる。

【0066】

【発明の効果】以上説明したように、請求項1に記載の発明によれば、従来で行われた暗号強度評価方法を行うことができる装置を実現することができる。

【0067】請求項2に記載の発明によれば、複数種のLSIを1つのLSIにまとめることにより、装置内の部品点数を減らすことができ、装置の小型化を図ることができる。また、1つのLSIを開発すればよいので、その開発コストを低減できる。

【0068】請求項3に記載の発明によれば、連想記憶メモリを使用することで、ハッシュ等の処理を行わなくとも、短時間で、表の要素と暗号文の加工値とを比較することができる。

【0069】請求項4に記載の発明によれば、第2LSIに比較プロセッサが有する機能の回路を付加することにより、比較プロセッサを省略することができる。この

ため、装置の小型化を図ることができる。

【0070】請求項5に記載の発明によれば、各LSIを装置が強度評価する暗号に対応するように設定できるので、どの暗号に対しても、暗号強度評価を行うことができる。

【図面の簡単な説明】

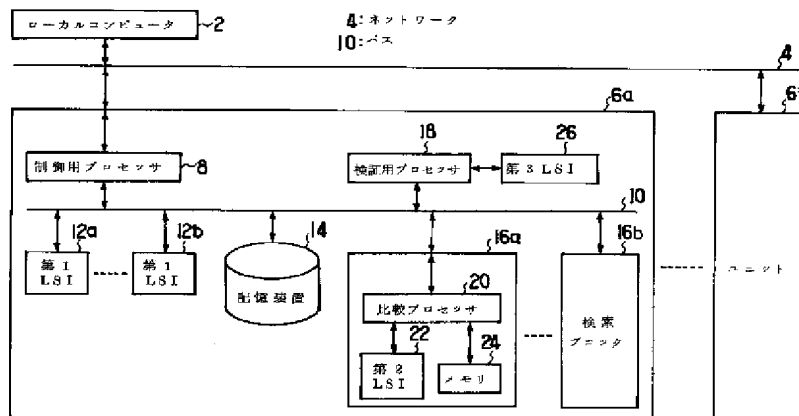
【図1】 本発明の実施の形態である暗号強度評価装置を示すブロック図である。

【図2】 本発明の実施の形態である暗号加工回路を示すブロック図である。

【符号の説明】

2 ローカルコンピュータ、4 ネットワーク、6a、6b ユニット、8制御用プロセッサ、10 バス、12a、12b 第1LSI、14 記憶装置、16a、16b 検索ブロック、18 検証用プロセッサ、20 比較プロセッサ、22 第2LSI、24 メモリ、30 暗号化回路、32 縮退化回路、34、36、38 セレクタ。

【図1】



【図2】

